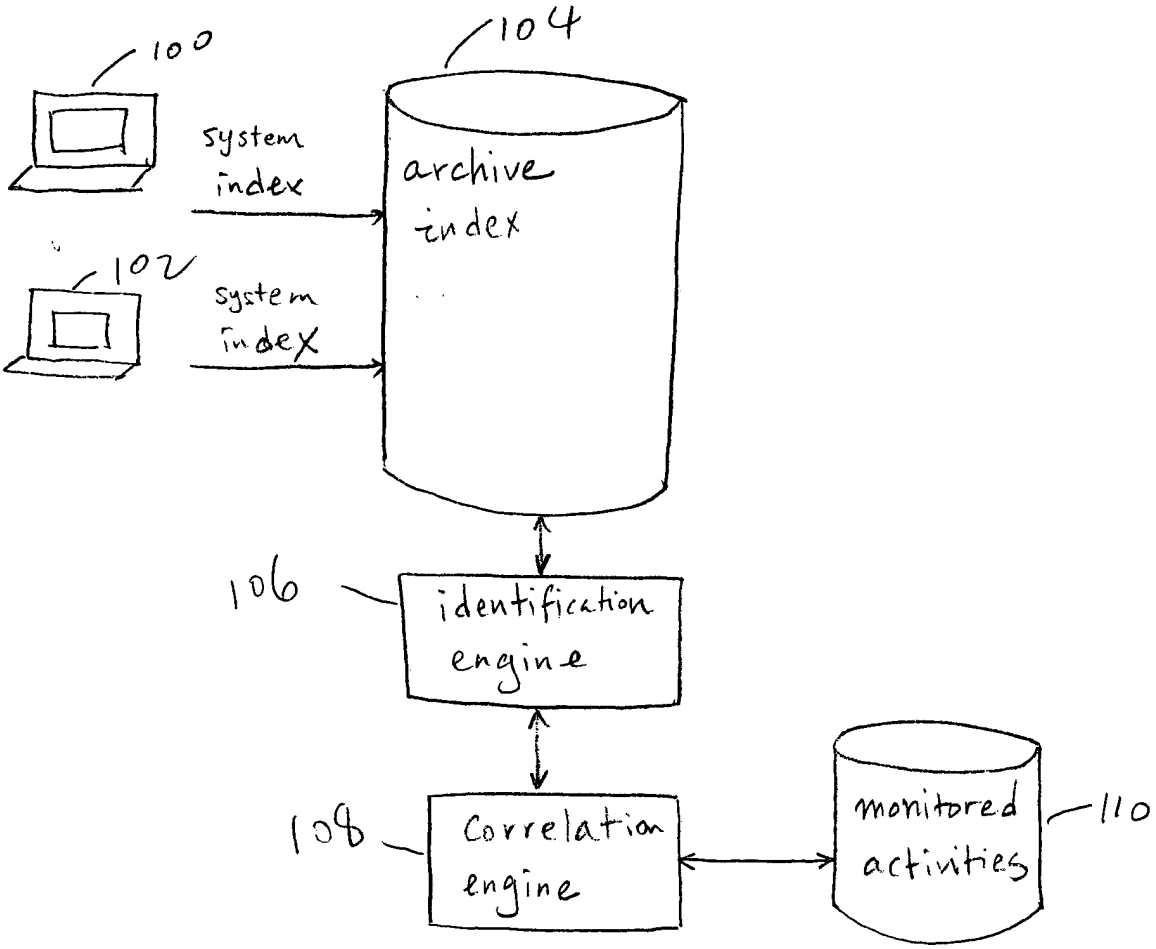
100
104
system index
archive index
102
system index
106
identification engine
108
Correlation engine
monitored activities
110

Figure 1

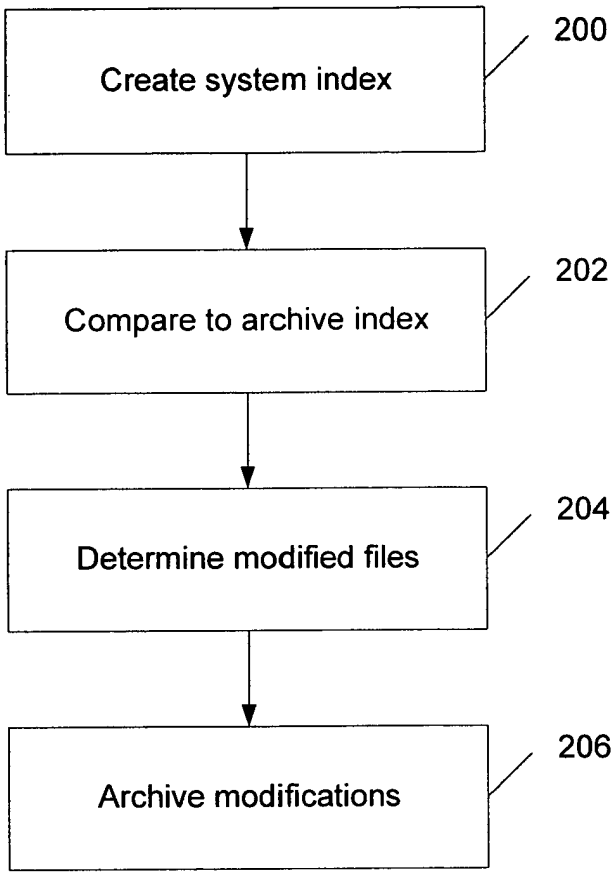
Create system index
200
Compare to archive index
202
Determine modified files
204
Archive modifications
206

Figure 2

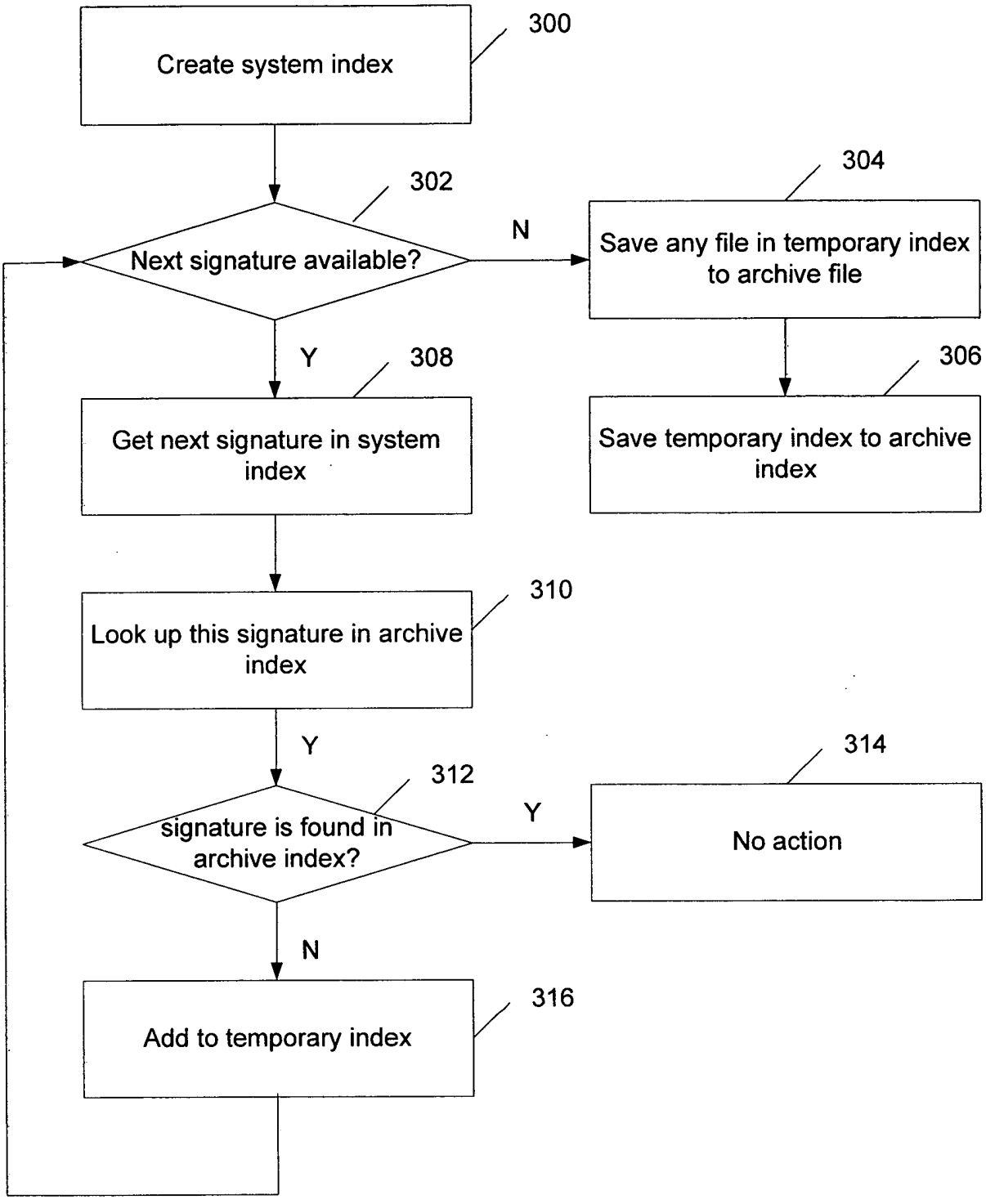
Create system index
300
302
Next signature available?
N
304
Save any file in temporary index to archive file
Y
308
Get next signature in system index
306
Save temporary index to archive index
310
Look up this signature in archive index
Y
312
signature is found in archive index?
Y
314
No action
N
316
Add to temporary index

Figure 3

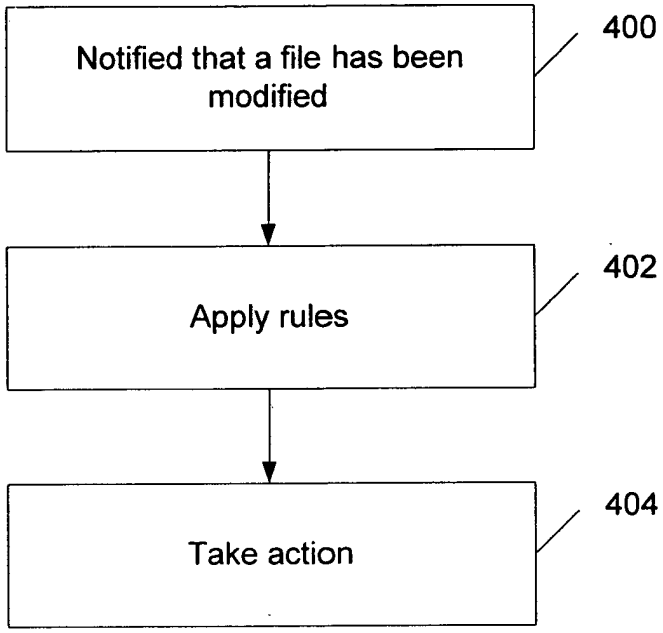
Notified that a file has been modified
400
Apply rules
402
Take action
404

Figure 4

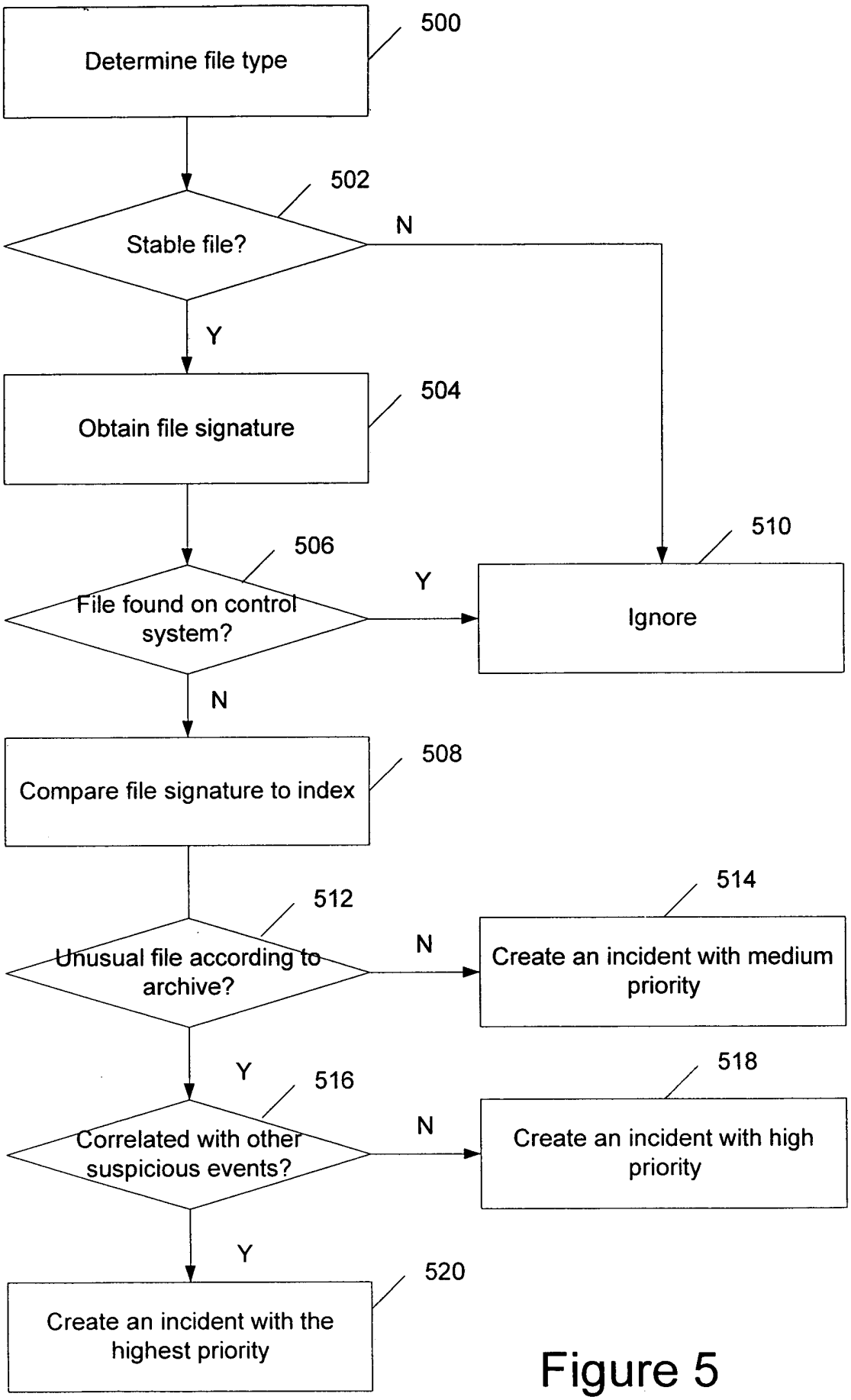
Determine file type
500
Stable file?
502
N
Y
Obtain file signature
504
File found on control system?
506
Y
Ignore
510
N
Compare file signature to index
508
Unusual file according to archive?
512
N
Create an incident with medium priority
514
Y
Correlated with other suspicious events?
516
N
Create an incident with high priority
518
Y
Create an incident with the highest priority
520

Figure 5